Revised Expanded Abstract (CyRes focussed)

Title: Strengthening Satellite Infrastructure with Cyber Resilience: Practical Adoption of CyRes for Trusted, Recoverable Space Systems

Expanded Abstract:
As small satellite missions evolve from experimental platforms into operationally critical infrastructure, cybersecurity must extend beyond protection and prevention toward full-spectrum cyber resilience. Constellation-scale deployments, software-defined payloads, and continuous in-orbit updates are increasing system complexity while simultaneously expanding the attack surface across spacecraft, ground segments, and globally distributed supply chains. In this environment, the ability not only to defend systems but to detect compromise and reliably recover to a known good state becomes mission critical.

The Trusted Computing Group's Cyber Resilient (CyRes) architecture provides a structured, standards-based approach to addressing these challenges. Rather than focusing solely on perimeter defenses, CyRes introduces a device-centric resilience model built on the principles of protection, detection, and recovery, enabling systems to maintain operational integrity even when components are compromised.

At the core of CyRes is the concept of the Cyber Resilient Module (CRM), an architectural construct that separates a potentially compromised Resilience Target (RT) from a protected Resilience Engine (RE), governed by an external Resilience Authority (RA). This separation ensures that even if mission software, firmware, or configuration is altered or corrupted, the RE retains the ability to restore the system deterministically and autonomously.

This model is particularly well aligned with the operational realities of small satellite missions, where physical access is impossible post-launch and communication windows may be intermittent. CyRes enables local, trusted recovery capabilities that do not rely on continuous connectivity, allowing spacecraft to detect anomalies, initiate recovery actions, and re-establish trusted operation independently.

CyRes is implemented through a set of Cyber Resilient Building Blocks (CRBBs) that provide low-level, hardware-enforced capabilities, including Protection Latches and Secure Execution Environments (SEE). Together, these mechanisms ensure that recovery processes themselves remain tamper resistant and reliable, addressing a key limitation of traditional security models.

Importantly, CyRes does not operate in isolation. It is designed to integrate with broader trusted computing technologies such as hardware Roots of Trust, device identity frameworks, and remote attestation mechanisms. Technologies like the Trusted Platform Module (TPM) and Device Identifier Composition Engine (DICE) provide foundational identity and measurement capabilities, while CyRes extends these into a complete lifecycle resilience framework, ensuring not just that a system can be trusted, but that it can remain trustworthy over time despite attack or failure.

For small satellite ecosystems, this approach directly addresses key challenges:

- Supply chain assurance through verifiable integrity of components and firmware prior to launch
- Operational resilience through autonomous detection and recovery from in-orbit compromise
- Interoperability through standardized mechanisms enabling multi-vendor systems to participate in a unified trust framework
- Lifecycle security supporting long-duration missions where updates and recovery must be efficient and deterministic

By embedding CyRes principles into spacecraft design, operators can move from reactive security models to proactive, recoverable systems capable of sustaining mission operations under adverse conditions.

This presentation will focus on the practical adoption of CyRes within small satellite architectures, including reference design patterns, integration with existing trusted computing technologies, and phased implementation strategies. It will demonstrate how CyRes can be applied to deliver verifiable, resilient, and recoverable space systems, enabling mission assurance at scale while preserving the flexibility and innovation that define the small satellite sector.